QUESTIONS & ANSWERS
RFQ #DOC52PAPT0601007

Q1: I notice the absence of the number of copies of the RFQ USPTO is requesting.

A1: This omission was inadvertent. The USPTO requests one original copy of the offeror's response to the RFQ and 3 copies.

Q2: Am I correct in assuming the extended price request is just the total value of the CLIN – unit value times the number of hours?

A2: Yes.

Q3: Is it appropriate/OK to cut & paste the representations and certifications from the RFQ in to my submission?

A3: No. See the first paragraph of 52.212-3 (on page 3). Representations & certifications must be completed electronically at http://orca.bpn.gov.

Q4: In the portion of the SOW which describes the Tri-Way initiative, coordination of the patent process by the EPO, JPO and USPTO is outlined. Is international travel by contractor personnel anticipated within the scope of this contract?

A4: Yes. See third paragraph ("Travel") on page 3.

Q5: Is all work associated with this contract to be performed at the USPTO? If not, what percentage of the work will be performed on-site?

A5: We anticipate that work will be performed both at the USPTO and at the contractor's location. We estimate a 50-50 split.

Q6: Will the USPTO furnish the contractor with on-site office space? What equipment will be provided by the government for on-site work?

A6: We will make an office available (with standard office equipment) on site at the USPTO as necessary.

Q7: What data security measures are to be observed by the contractor when working off-site? Will the government furnish the contractor with a secure line, secure computer, unique software and/or encryption for remote access?

A7: We do not anticipate providing access to sensitive or classified information at this time and will not provide the items listed above. However, the RFQ is hereby modified to include the following security clauses:

ACCESS TO GOVERNMENT FACILITIES

During the life of the contract, the rights of ingress and egress to and from the Government facility for Contractor personnel shall be made available as required per each individual task order. During all operations on Government premises, Contractor personnel shall comply with the rules and regulations governing the conduct of personnel and the operation of the facility. The Government reserves the right to require Contractor personnel to sign in upon ingress and sign out upon egress to and from the Government facility.

DUPLICATION AND DISCLOSURE OF CONFIDENTIAL DATA

Duplication or disclosure of confidential data provided by the USPTO or to which the Contractor will have access as a result of this contract is prohibited. It is understood that throughout performance of the contract the Contractor may have access to confidential data which is the sole property of the USPTO, as well as access to proprietary data which is the sole property of other than the contracting parties. The Contractor hereby agrees to maintain the confidentiality of all such data to which access may be obtained throughout contract performance whether title thereto vests in the USPTO or otherwise. The Contractor hereby agrees not to disclose said data, any interpretations thereof or data derivative therefrom, to unauthorized parties in contravention of these provisions without prior written approval of the CO or the party in which title thereto is wholly vested. This clause also applies to any subcontractors and/or consultants used by the Contractor.

GOVERNMENT FURNISHED DATA (IF APPLICABLE)

The Government shall deliver to the Contractor, as may be requested, Government-Furnished Data (GFD) during the performance of this contract. GFD will be delivered to the Contractor as specified in each task order.

Title to GFD shall remain in the Government, and the Contractor shall use the GFD only in connection with this contract.

Upon completion or termination of this contract, the Contractor shall return to the Government all GFD.

RIGHTS IN DATA (IF APPLICABLE)

The Government shall have unlimited rights in software first produced in the performance of this contract. For the purposes of this clause, "software first produced in the performance of this contract" shall include, but not be limited to the following: non-COTS computer programs developed or previously developed and implemented by the Contractor in the performance of this contract, related computer data bases and documentation thereof, source code, object code, algorithms, library code, library routine, and technical data of all software first produced in the performance of this contract. For the purposes of this clause, "unlimited rights" shall mean the right of the USPTO, at no extra cost to the USPTO or recipients, to use, disclose, reproduce unlimited copies, prepare derivative works, distribute unlimited copies to the public and foreign government patent offices, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

SECRECY AND USAGE OF PATENT INFORMATION

Work under this contract does not affect the national security. However, patent applications are required by law (35 U.S.C. 122) to be kept in confidence. Information contained in any patent application file(s) is restricted to authorized Contractor personnel on a need-to-access basis.

The Contractor acquires no right or privilege to use or disclose any information contained in any patent application file (in any form whatsoever) except to perform the work under the contract. Further, the Contractor shall not copyright or make any use or disclosure whatsoever of any patent information contained in any application or related copy or data furnished the Contractor by the Government or obtained therefrom except performing the requirements of this contract.

Security requirements of patent application file data maintained in a computer-accessible medium are an extension of the security requirements for the hard copy or the patent application folders. All processing, storage or transmission of patent application file data by means of electronic communications systems is prohibited unless use of such systems is approved by the USPTO.

All personnel having access to patent application files or data or information concerning the same, must take the following at or affirmation, signed in writing:

"I do swear or affirm that I will preserve the applications for patents in secrecy, that I will not divulge any information concerning the same to unauthorized persons while employed in work under this contract or at any time thereafter; and that I take this obligation freely, and without mental reservation or purpose of evasion."

Each employee's signed oath, or affirmation, shall be retained in the Contractor's file, subject to inspection by authorized Government representatives.

Without advance notice, the Government shall have the right to inspect the Contractor's premises, records, and work in process pertaining to the secrecy of patent information.

CAR 1352.239-73 SECURITY REQUIREMENTS FOR INFORMATION TECHNOLOGY RESOURCES (OCTOBER 2003) (Modified)

(a) This clause is applicable to all contracts that include information technology resources or services in which the Contractor must have physical or electronic access to USPTO's sensitive or classified information, which is contained in systems that directly support the mission of the Agency. For purposes of this clause, the term "Sensitive" is defined by the guidance set forth in:
(1) The DOC IT Security Program Policy and Minimum Implementation Standards http://www.osec.doc.gov/cio/ITSIT/DOC-IT-Security-Program-Policy.htm;
(2) The Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources (http://csrc.nist.gov/policies/appendix_iii.pdf), which states that there is a "presumption that all [general support systems] contain some sensitive information."; and
(3) The Computer Security Act of 1987 (P.L. 100-235) (http://www.epic.org/crypto/csa/csa.html), including the following definition of the term sensitive information "…any information the loss, misuse, or unauthorized access, to or modification of which could adversely affect the national interest or the, conduct of federal programs, or the privacy to which individuals are entitled under section 552 of title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

For purposes of this clause, the term "Classified" is defined by the guidance set forth in:
(1) The DOC IT Security Program Policy and Minimum Implementation Standards, Section 3.3.1.4 (http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf).
(2) The DOC Security Manual, Chapter 18 (http://www.easc.noaa.gov/Security/webfile/erso.doc.gov/5_2003%20Security%20Manual/DOC%20Manual%20of%20Security%20Policies%20and%20Procedures.htm).
(3) Executive Order 12958, as amended, Classified National Security Information. Classified or national security information is information that has been specifically authorized to be protected from unauthorized disclosure in the interest of national defense or foreign policy under an Executive Order or Act of Congress.

Information technology resources include, but are not limited to, hardware, application software, system software, and information (data). Information technology services include, but are not limited to, the management, operation (including input, processing, transmission, and output), maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. The Contractor shall be responsible for implementing sufficient Information Technology security, to reasonably prevent the compromise of USPTO IT resources for all of the contractor's systems that are interconnected with a USPTO network or USPTO systems that are operated by the Contractor.

(b) All Contractor personnel performing under this contract and Contractor equipment used to process or store USPTO data, or to connect to USPTO networks, must comply with the requirements contained in the USPTO IT Security Handbook.

(c) For all Contractor-owned systems for which performance of the contract requires interconnection with a USPTO network or that USPTO data be stored or processed on them, the Contractor shall:

(1) Provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall comply with federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq,) and the Federal Information Security Management Act of 2002, Pub. L. No. 107-347 Stat. 2899, 2946-2961 (2002); Pub. L. No. 107-296 Stat. 2135, 2259-2273 (2002). 38 WEEKLY COMP. PRES. DOC. 51,2174 (Dec. 23, 2002) (providing statement by President George W. Bush regarding Federal Information Security Management Act of 2002). The plan shall meet IT security requirements in accordance with Federal and USPTO policies and procedures that include, but are not limited to:

(a) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources (http://csrc.nist.gov/policies/appendix_iii.pdf);
(b) National Institute of Standards and Technology Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-18/Planguide.PDF); and
(c) DOC Procedures and Guidelines in the Information Technology Management Handbook (http://nsi.org/Library/Govt/docinfo.txt).
(d) National Industrial Security Program Operating Manual (NISPOM) for classified systems (http://www.dss.mil/isec/nispom.htm); and

(2) Upon award, the contractor shall register with the USPTO Certification and Accreditation Group (CACG), with copy to the Contracting Officer, to initiate the certification and accreditation process described in paragraph 3 below.

(3) Within 14 days after receipt of direction from the CACG, the contractor shall submit for USPTO approval a System Certification and Accreditation package, including the IT Security Plan and a system certification test plan, as outlined in USPTO Certification and Accreditation Technical Standard and Guideline. The Certification and Accreditation Package must be consistent with and provide further detail for the security approach contained in the offeror's proposal or sealed bid that resulting in the award of this contract and in compliance with the requirements stated in this clause. The Certification and Accreditation Package, as approved by the Contracting Officer, in consultation with the USPTO Security Officer, shall be incorporated as part of the contract. USPTO will use the incorporated IT Security Plan as the basis for certification and accreditation of the contractor system that will process USPTO data or connect to USPTO networks. Failure to submit and receive approval of the Certification and Accreditation Package, as outlined above may result in termination of the contract.

(d) The Contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

CAR 1352.239-74 SECURITY PROCESSING REQUIREMENTS FOR CONTACTOR/SUBCONTRACTOR PERSONNEL FOR ACCESSING USPTO AUTOMATED INFORMATION SYSTEMS (OCTOBER 2003)

(a) Contractor personnel requiring any access to AIS's operated by the Contractor for USPTO or interconnected to a USPTO network to perform contract services shall be screened at an appropriate level in accordance with Commerce Acquisition Manual 1337.70, Security Processing Requirements for Service Contracts. USPTO shall provide screening using standard personnel screening forms, which the Contractor shall submit to the USPTO Contracting Officer's Technical Representative (COTR) based on the following guidance:

1) Contract personnel performing work designated Contract High Risk and personnel performing work designated Contract Moderate Risk in the information technology (IT) occupations and those with "global access" to an automated information AIS require a favorable pre-employment check before the start of work on the contract, regardless of the expected duration of the contract. After a favorable pre-employment check has been obtained, the Background Investigation (BI) for Contract High Risk and the Minimum Background Investigation (MBI) for Contact IT Moderate Risk positions must be initiated within three working days of the start of work.

2) Contract personnel performing work designed Contract Moderate Risk who are not performing IT-related contract work to not require a favorable pre-employment check prior to their employment; however, the Minimum Background Investigation (MBI) must be initiated within three working days of the subjects start of on the contract, regardless of the expected duration of the contract.

3) Contract personnel performing work designated as Contract Low Risk will require as National Agency Check and Inquiries (NACI) upon the subjects start of work on the contract if the expected duration of the contract exceeds 365 calendar days. The NACI must be initiated within three working days of the subjects start of work on the contract.

4) Contract personnel performing work designated Contract Low Risk will require a Special Agreement Check (SAC) upon the subject's start of work on the contract if the expected duration of the contract (including options) exceeds 180 calendar days, but is less that 365 calendar days. The SAC must be initiated within three working days of the subject's start of work on the contract.

5) Contract personnel performing work on contracts requiring access to classified information must undergo investigative processing according to the Department of Defense National Industrial Security Program Manual (NISPOM), (http://www.dss.mil/isec/nispom.htm) and be granted eligibility for access to classified information prior to beginning work on the contract.

The security forms may be obtained form USPTO Office of Security. At the option of the government, interim access to USPOT AISs may be granted pending favorable completion of a pre-employment check. Final access may be granted only on a completion of an appropriate investigation based upon the risk level assigned to the contract.

(b) Within 5 days of contract award, the Contractor shall certify in writing to the COTR that it's employees, in performance of the contract, have completed annual IT security awareness training in USPTO IT Security policies, procedures, computer ethics , and best practices, in accordance with the USPTO Training Policy. The COTR will inform the Contractor of any other available USPTO training resources.

(c) Within 5 days of contract award, the Contractor shall provide the CORS with signed Nondisclosure Agreements as specified in Commerce Acquisition Regulations (CAR), 1352.209-72, Restrictions Against Disclosures.

(d) The Contractor shall afford USPTO, including the Office of Inspector General, access to the Contractor's and subcontractors facilities, installations, operations, documentation, databases, and personnel used in performance of the contract. Access shall be provided to the extent required to carry our a program of IT inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of USPTO data or to the function of computer AISs operated on behalf of USPTO, and to preserve evidence of computer crime.

(e) The Contractor shall incorporate this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(NOTE: Low Risk contracts whose duration if less than 180 days do not ordinarily required security processing. However, even though the contract is short in duration, based on any unusual circumstances that may exist, Special Agreement Checks (SACs) may be requested, at the discretion of the Contracting Officer's Technical Representative (COTR) and/or the USPTO Security Office.)

Q8: Has the USPTO contracted for expert advice and recommendations related to rule package changes and quality improvements prior to the issuance of this RFQ?

A8: No.

Q9: What has been budgeted by the USPTO for the consulting tasks outlined in this RFQ?

A9: As mentioned, the USPTO does not have experience in contracting for these specialized services and therefore does not wish to limit offerors by setting an arbitrary number. We will evaluate RFQ responses in accordance with the methodology & weighting outlined in the RFQ.